Wat is Active Directory en wat houd het in?

Heb je wel eens nagedacht over het feit hoe een (systeem) beheerder op school en / of werk de zaakjes in handen heeft? Bijvoorbeeld, hoe is het mogelijk dat je met je eigen account op elke computer kan inloggen en je eigen bestanden altijd beschikbaar zijn? (Uitzonderingen daargelaten) Naast andere middelen wordt er ook gebruik gemaakt van Active Directory. To the point: Wat is nu precies Active Directory, en wat kan ik ermee?

Active Directory werd geïntroduceerd bij het verschijnen van Windows server 2000. Ook in zijn opvolger, Windows server 2003 is Active Directory geïmplementeerd. Op moment van schrijven bestaat Windows server 2008 al en ook daarin is Active Directory verreweg het belangrijkste onderdeel van dit netwerkbesturingssysteem.

Beveiliging:
Een netwerk heeft vooral de taak diensten te verlenen aan een gebruiker. Denk hierbij aan data sharing enzovoorts. Daarnaast speelt beveiliging een grote rol en is één van de belangrijkste bestaandsgronden voor client / server netwerken. In dit artikel twee soorten beveiliging:

- Verificatie
- Autorisatie

Verificatie en autorisatie zijn begrippen waar je ook in het dagelijkse leven mee geconfronteerd wordt. Als je bijvoorbeeld in een vliegtuig stapt, moet je daarvoor toestemming hebben: Autorisatie. Voor het vertrek moet je kunnen aantonen dat je op je eigen ticket reist en niet op die van iemand anders: Verificatie.

Verificatie:
Verificatie wordt gebruikt als toegangsbeveiliging tot het netwerk. Van jij als gebruiker worden bepaalde gegevens op het netwerk bewaard in een zogeheten user-account. Voor de verificatie zijn dat onder andere je gebruikersnaam en wachtwoord.

Autorisatie:
Autorisatie wordt gebruikt als toegangsbeveiliging voor een netwerk object dat aan jouw als gebruiker beschikbaar is gesteld. Elk netwerk object is voorzien van een ACL (Access Controll List). In de ACL zijn de toegangspermissies per netwerk object vastgesteld. De toegang via de ACL's wordt geregeld via SID's (Security Identifier) Een SID is een unieke waarde van je gebruikersaccount. (Bij het creëren van een account wordt een SID toegekend) Een SID met de daarbijbehorende toegangspermisies heet een ACE (Access Controll Entry). Dat betekend dus dat er in een ACL verschillende ACE's kunnen voorkomen. Kortom via de autorisatie wordt dus geregeld of en zoja hoe jij als geverifieerde gebruiker van de netwerk objecten gebruik mag maken.

Structuur van een Active Directory server:
Een Active Directory server kan onder andere de volgende attributen bevatten:

- Domeinen
- Sites
- Trees

- Forests
- Trusts

Deze bovenstaande attributen hieronder breder uitgewerkt:

Domeinen:
Een domein is een verzameling gebruikers en computers met een gemeenschappelijk beveiligingsbeleid. Een domein wordt dan ook als een éénheid beheerd. Even een weetje voor je verder gaat:

Onder Windows NT4 Server was het gebruikelijk dat de geografische spreiding van een organisatie model stond voor het netwerk. Per locatie was er dus een domein. Het beheer was dus min of meer gedecentraliseerd. Via ingewikkelde modellen en methodes werden de verschillende domeinen in één structuur ondergebracht. Je zal je hoogstwaarschijnlijk afvragen waarom dit? En niet alles centraal? De belangrijkste reden om verschillende domeinen te hanteren was de beperkte capaciteit. Officeel konden er 'maar' 100.000 gebruikers in een domein worden opgenomen. Echter, in de praktijk bleek dat er boven ongeveer de 20.000 er al problemen ontstonden. Grote ondernemingen waren dus genoodzaakt het beheer gedecentraliseerd te organiseren. De capaciteit is vandaag de dag gelukkig geen probleem meer. Miljoenen gebruikers kunnen er nu in een domein worden opgenomen. (De grens is nog steeds niet ontdekt)

Sites:
Een site is een geografische eenheid, een locatie. Een domein is een **logische** eenheid van gebruikers en computers, een site een **fysieke**. Je kan je waarschijnlijk wel voorstellen dat een bedrijf één domein heeft waarbij de kantoren op twee verschillende locaties staan. In dat geval is het domein verspreid over twee sites. Omgekeerd is het mogelijk om direct na een bedrijfsovername twee domeinen op één locatie te hebben. Dan zijn er twee domeinen in één site.

Trees:
Een tree is niets anders dan een hiërarchische domeinstructuur. Dat is te verdelen in de volgende attributen:

- Root domein
- Parent domein
- Child domein

De domeinnamen in een tree vormen een Contiguous namespace, een aangrenzende naamruimte. Behalve het Root Domain heeft elk ander domein een eigen naamdeel, gevolgd door de naam van het Parent domain.

Forests:
Elke organisatie moet zich kunnen beschermen tegen de buitenwereld. In Active Directory bestaat de bescherming onder andere uit de verzameling user-accounts van alle bedrijfsdeelnemers. Ik heb al eerder verteld dat een domein kan worden beschouwd als de kleinste standaard beveiligingseenheid binnen een organisatie. Ik heb ook al verteld dat organisaties verschillende domeinen kunnen hebben, ondergebracht in één of meerdere trees. Een forest kan worden beschouwd als de grootste beveiligingseenheid binnen Active Directory. Een forest bakent de beveiliging van de gehele organisatie af. Een forest kan

bestaan uit één of meerdere domeinen. De belangrijkste eigenschap van een forest is dat verschillende domeinen elkaar vertrouwen. Hierdoor kunnen alle bedrijfsonderdelen met elkaar samenwerken. Alles wat niet tot de forest behoort, wordt dus niet vertrouwd en kan geen toegang krijgen tot de netwerkobjecten.

Trusts:
Een vertrouwensrelatie tussen domeinen wordt een Trust relationship of korter Trust genoemd. Via een trust wordt het mogelijk dat gebruikers uit het ene domein kunnen beschikken over bronnen uit het andere domein. Voorbeeld: Wanneer je een printer uit een ander domein wilt gebruiken moet er tussen het domein waar je nu in zit en het andere domein een Trust relationship bestaan.

Active Directory zelf:
De gegevens van alle netwerkobjecten moeten ergens op het netwerk worden opgeslagen. Wanneer dit niet gebeurd kan er bijvoorbeeld niet worden geverifieerd of geautoriseerd en werkt de netwerkbeveiliging niet. Al deze gegevens worden bewaard in het bestand NTDS.DIT. NTDS is een afkorting van New Technology Directory Service. DIT is een afkorting van Data Information Table. Het bestand NTDS.DIT wordt dus Active Directory genoemd. Een Windows server waarop Active Directory is geïnstalleerd, heet een Domain Controller. Active Directory NTDS.DIT is dus een databasebestand. Het bestand wordt bewerkt met een databaseprogamma. In Windows server wordt dat gedaan door het databaseprogramma: directories. Het databaseprogramma plus Active Directory worden samen de Directory Service genoemd.

Active Directory is zo ontworpen dat het naadloos aansluit bij de geldende Internet-standaarden. Zo heeft Active Directory onder ander het Domain Name System (DNS) nodig om goed te kunnen functioneren. Voor deze tutorial is het voldoende als je weet dat DNS ervoor zorgt dat een computer in het netwerk via zijn naam kan worden opgespoord. (Het is dus noodzakelijk dat computernamen uniek zijn)

De Global Catalog:
In uitgebreide domeinstructuren kost het erg veel tijd en netwerkcapaciteit om informatie uit een domein op te halen. (Denk aan een domein wat in een andere tree van een forest ligt) Daarom gebruikt Active Directory de Global Catalog. Een Global Catalog wordt op één of meerdere Domain Controllers bewaard. Die Domain Controllers zijn dan Global Catalog Servers (GCS). Per definitie is de eerste Domain Controller van het eerste domein van de eerste tree in een forest een GCS. De Global Catalog is een database waarin de volgende attributen worden opgeslagen:

- Van alle objecten uit het eigen domein worden de eigenschappen bijgehouden.
- Van alle objecten uit de overige domeinen wordt een deel van de eigenschappen bijgehouden.

Van gebruikers uit het eigen domein worden alle eigenschappen bijgehouden. Bij de gebruikers uit de overige domeinen is dat alleen de gebruikersnaam, de voornaam, de achternaam en het wachtwoord. Via een replicatieproces wordt de Global Catalog op de Global Catalog Servers gelijk gehouden.

Objectgeoriënteerd:

Active Directory werkt objectgeoriënteerd. Objecten moeten gedefinieerd zijn. Dat definiëren begint bij het Active Directory schema. Het Active Directory Schema is een verzameling definities. In het Schema bestaan twee soorten definities:

- Attributen.
- Objectklassen.

In een attribuut wordt een kenmerk gedefinieerd. Elk attribuut wordt maar één keer gedefinieerd. Daarbij is ook het type van de informatie vastgelegd.

Een objectklasse bestaat uit een aantal attributen die ook in het Schema zijn gedefinieerd. Een objectklasse werkt als een sjabloon. Door een instantie van een objectklasse te creëren, wordt een daadwerkelijk object gemaakt. Dat object erft de attributen uit de desbetreffende objectklasse. De attributen van het object bevatten de informatie die het object beschrijven: De attribuutwaarden. Wanneer je met Window Server werkt kan je ze terug zien in het propertie-venster van het object als de object-properties: De eigenschappen in het eigenschappen venster.

Elk object in Active Directory wordt gekarakteriseerd via zijn GUID. GUID is een afkorting van Global Unique Identifier. De GUID is een nummer van 128 bits. Elk object krijgt bij het creëren ervan een GUID. Het zoeken naar objecten in Active Directory gaat met behulp van GUIDs.

Standaard objectklassen:
Nu je weet hoe objecten in Active Directory tot stand komen, bespreek ik de belangrijkste standaard ingebouwde objectklassen.

Users:
Voor elke gebruiker in Active Directory moet een user-object worden aangemaakt door een instantie te creëren van de betreffende objectklasse. Bij dat aanmaken moet je tenminste de User logon name van het (voorlopige) Password invoeren. De User logon name wordt ook wel de accountnaam / gebruikersnaam genoemd. Later kan je nog een groot aantal andere eigenschappen toekennen. Een aantal daarvan behandel ik in een aantal hoofdstukken hierna. Een gebruiker is een Security principal en kan dus via zijn SID voorkomen in ACE's van de ACL's van netwerkobjecten zoals ik al eerder verteld heb.

Computers:
Voor elke computer die lid wordt van een domein wordt een computer-account aangemaakt. Je creëert daarbij een instantie van de desbetreffende objectklasse. Een computer moet een unieke Computer name hebben. Ook een computer is een Security principal zodat deze een eigen SID heeft.

Groepen:
Een groep maak je door een instantie te creëren van de objectklasse Group. In een groepobject breng je gebruikers-accounts en/of computer-accounts onder in een logische eenheid. In veel gevallen kan een groep zelf ondergebracht worden in andere groepen. Van groepen bestaan twee categorieën. De Security groups zijn Security principals en bezitten een eigen SID. En Distribution groups zijn dat niet. Groepen hebben betrekking op een scope, een reikwijdte. Op Domain Controllers kunnen de volgende soorten groepen voorkomen:

- Universal groups.
- Global groups.
- Domain local groups.

In één van de volgende hoofstukken kan je hier mee over lezen.

Organizational Units:
Een Organizational Unit (OU) is een containerobject. Een Organizational Unit herbergt objecten uit het eigen domein. Een Organizational Unit kan de volgende objecten bevatten:

- Users.
- Computers.
- Gedeelde bronnen (Schijven, folders en printers).
- Applicaties.
- Andere Organizational Units.

Organizational Units zijn de kleinste eenheden waarvan je beheertaken kan delegeren. Op een Organizational Unit kan je Group Policies toepassen. Met Organizational Units kan je binnen een domein een structuur opzetten die lijkt op een organisatorische structuur van een bedrijf. Daardoor wordt het beheer realistischer en daarmee eenvoudiger. Organizational Units zijn geen Security principals